ABSTRACT

This invention relates to a method for enabling the use of valid authentication certificates when the public key and private keys of any of the certifying authority have expired, comprising obtaining a server certifying authority chain (SCAC) certificate by the server from the said certifying authority, presenting the original valid authentication certificate along with the said server certifying authority chain certificate by the server to the browser during the SSL handshake, accepting the transaction by the browser after verification of the original authentication certificate using the expired public key of the certifying authority, and verifying the said SCAC certificate using the new public key of the said certifying authority.

This invention further includes a system conducting secure transactions including a certifying authority for authenticating such transactions.